# Kiteworks + BigID

Extend Data Modernization, Governance, and Control Beyond the Enterprise



## Leverage BigID Automatic Data Classification to Mitigate Risk of Data in Motion and in Use

BigID discovers and classifies sensitive data wherever it lives, automatically identifying PII, PHI, financial data, and other sensitive information across your data landscape. BigID surfaces risk scores, data lineage, and overexposure insights. But as data moves beyond your perimeter through email, file sharing, APIs, and MCP, maintaining that visibility and control requires downstream enforcement.

The Data Policy Engine at the heart of the Kiteworks Private Data Network **consumes BigID's data sensitivity labels** and risk intelligence and enforces consistent, auditable governance over how sensitive documents are shared, accessed, and used downstream—**even outside your organization.** It applies these policies to email, file sharing and collaboration, SFTP, MFT, and API-based automation.

#### How the Kiteworks Data Policy Engine Mitigates Downstream Risk

**BigID Classification Ingestion:** Automatically enforce policies on documents classified by BigID

**Risk-Based Access Controls:** Define policies that intake data attributes such as BigID sensitivity labels, user attributes such as role and location, and the user's action, such as edit or download, and enforce a run-time policy such as view-only, SafeEDIT, block, encrypt, or allow

**Possessionless Editing:** Enable secure document editing for internal and external users virtually in their browsers, without file downloads, with SafeEDIT next-gen DRM

**End-to-End Encryption:** Apply military-grade encryption for data in transit and at rest across email, file sharing, SFTP, APIs, and forms

**Unified Audit Logging and Reports:** Provide the SOC and compliance teams with comprehensive, real-time visibility into every access, share, and transfer event, including external data exchanges

### Solution Highlights



Automatically discovers, classifies, and labels data



Protects data in use, in motion, and at rest



Enforces even outside your enterprise



Possessionless editing for secure collaboration

Kiteworks + BigID SOLUTION BRIEF

#### Internal Environment **External Environment** Secure Data Exchange Data Discovery, Data **Email** Classification, Mapping and Labeling Partners & **Kitewarks** Customers **Agentic Risk** Risk **MFT and SFTP** Remediation Scoring Data Systems **Data Sources Policy Labeled Data Files** Sharing, DRM & **Engine** amazon SharePoint Collaboration Suppliers box (SEN ) wasabi splunk> Google Drive More.. **APIs and MCP** ArcSight**⋠** Any SIEM...

Diagram 1: Enforce policies using BigID data classifications.

#### **Automate Governance Without Sacrificing Business Process Responsiveness**

Kiteworks automatically enforces the right level of protection based on user roles, run-time context, and BigID sensitivity labels and risk scores. Business users collaborate seamlessly while high-risk activities are limited or blocked—without constant intervention from security teams. BigID's risk insights trigger automated protective actions in Kiteworks such as encryption, access restrictions, or SafeEDIT-only modes based on data sensitivity and user context.

#### **Extend BigID Data Security to Your Supply Chain**

Kiteworks extends the upstream benefits of BigID protection downstream into your supply chain by enforcing BigID's classification and risk-based controls on sensitive data shared externally. It ensures secure, compliant exchanges with vendors and partners—applying encryption, access policies, and audit logging to maintain your data security posture beyond the perimeter.

### **Turn BigID Insights Into Real-Time Action**

Together, BigID and Kiteworks bring discovery, classification, and enforcement together to deliver continuous protection across the entire data life cycle:

- Discover and classify sensitive data across all environments with BigID
- Enforce those classifications in motion and in use through Kiteworks' Data Policy Engine
- Turn BigID insights into real-time action to reduce exposure and risk
- Prevent overexposure and data leaks without slowing collaboration or workflows
- Close visibility gaps when data leaves internal systems and enters external channels

### **Simplify Compliance**

- Demonstrate control over regulated data flows (e.g., CUI, PCI, PHI, PII)
- Map activity to compliance frameworks like NIST CSF, GDPR, HIPAA, CMMC, CCPA, and ISO 27001
- Feed the unified audit log and dedicated reporting into compliance audits and incident response
- Achieve end-to-end visibility over sensitive data exchanges with irrefutable, centralized evidence for auditors

#### **Kitewarks**

Copyright © 2025 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a Private Data Network that delivers data governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and over 1,500 global enterprises and government agencies.